MINUTES OF THE COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD MEETING

JUNE 12-13, 1996

Wednesday, June 12, 1996

Introduction

A quorum being present, Dr. Willis Ware, Board Chairman, called the meeting to order at 9:00AM. In addition to Dr. Ware, the following Board members were present: Charlie Baggett, Jr., Genevieve Burns, Addison Fischer, Sandra Lambert, Joseph Leo, Gloria Parker, Randy Sanovic, George Spix, Linda Vetter and Rick Weingarten. The chairman recognized Mr. Weingarten and welcomed him as a new member to the Board.

Mr. Ed Roback, Board Executive Secretary, reviewed the agenda for the two-day meeting as well as the handout material that had been provided to the Board. Chairman Ware noted the special significance of the recent National Research Council study on cryptography and saw it as an accomplishment as related to the Board's resolution of March 1992 calling for a national level public review of the positive and negative implications of the widespread use of cryptography**.** Dr. Ware also discussed the results of his interactions with OMB with regard to the concerns expressed at the March meeting by Board members of sensed inconsistency in expectations between NIST and OMB regarding the mission of NIST pertaining to the implementation of A-130 (Appendix III).

Business Crypto Issues Update

Board member Sandra Lambert addressed the board on the current activities of the ICC/BIAC/OECD Business-Government Forum on Global Cryptography Policy. A meeting was held on May 7, 1996 in Washington, DC at which updates on crypto policy development from the governments of France, United Kingdom, European Community, United States, Japan and Germany were given. Some of the highlight areas discussed at this meeting were: government access issues, key management policies; self-escrow controversy; key storage and length of retention; certification of escrow agents; and certification of foreign agents. The emphasis was on stored records, not telephony. There was discussion that the limitation of cryptography in general would impede economies of companies and hamper the development of the GII.

Ms. Lambert also reported on a meeting of the Ad Hoc Group of Experts on Cryptography Policy Guidelines held on May 8, 1996 in Washington, DC. Attendees included EC, BIAC, OECD Secretariat, and government representatives from Australia, Austria, Canada, Denmark, France, Germany, Japan, Norway, Spain, Sweden, Turkey, United Kingdom and the United States. The mission of this group is to develop cryptography guidelines by February 1997. Board members expressed their concern about possible confusion between data communication references and how they are perceived, i.e., wire tapping, telephony. Lambert stated that the BIAC is interested in what the access requirements are and do not want specific technical specifications to be dictated. Another area of concern expressed at the meeting was about trusted third parties and whether key escrow is necessary. Companies expressed their fears of losing secure data within their own organization.

PKI Status

Donna Dodson of NIST gave a presentation on NIST's public key infrastructure program. She stated that there are four people at NIST concentrating on their efforts in this area. Ms. Dodson described the approach, PKI components and services and PKI implementation projects. She stated that Cooperative Research and Development Agreements (CRDAs) were been established with industry partners involved in PKI with NIST writing specifications for minimal interoperability. Listed among the invited PKI CRADA partners were AT& T, BBN, Certicom, Cylink, DynCorp, GTE, IRE, Motorola, Northern Telecom, Spyrus and Verisign. Chairman Ware stated that given the projected progress of this effort, it appeared to him that it would perhaps be the year 2000 before the government would have any significant results. Dodson confirmed that the year 2000 was a close estimate, but indicated that it was not just government but that industry was also lagging. This in part is due to industry not being certain if it will have the products to meet the PKI approach even if buyers would have the funds to spend. Sandy Lambert mentioned that the X9 standards arena has standards in place on certification authority and that while the standards will be done shortly, and robust technical implementation will follow. Lambert believes that business will be ahead of the government, however, with France looking at having certification by the end of 1996 with Canada and Japan not far behind. It was also pointed out that as a result of a recent GITS working group effort, 20-25 identified agency projects were working on a PKI interoperability effort.

Enabling Privacy, Commerce, Security and Public Safety on the Global Information Infrastructure

Bruce McConnell, OMB, and co-chair of the Interagency Working Group on Cryptography Policy addressed issues raised as a result of the draft white paper produced by this working group. McConnell commended the CSSPAB for having the foresight to

call for a national debate on this topic as evidenced by the Board's earlier resolution. He stated that the basic approach of the Administration was that they understand the need for strong cryptography and believe it to be a valuable component necessary to realize electronic commerce. However, he pointed out that the law enforcement community has concerns with the uncontrolled use of encryption as they relate to hiding criminal activities. The report suggests having a key management infrastructure (KMI) to include key recovery, as firms will want to go back and retrieve information that has been encrypted. KMI would be voluntary and designed and operated by the private sector. He emphasized that they are not talking about escrow of signature keys but keys used for confidentiality. Operational testing is needed to address scalability and interoperability issues. Mr. McConnell indicated that the State Department would be in a position to be part of a test pilot involving international communications. Other agencies would be needed for the pilot projects as well. The standards effort also needs to be worked. The government, specifically NIST, will be working with industry to develop a draft standard for government use and to ensure it fits with other cryptographic-based standards. They recognize that technology is not there yet; that there is no key recovery system in place yet. While industry is interested, its short term problem is in marketing non-escrowed software/hardware encryption overseas. Mr. McConnell said that the NRC report was an excellent service provided by private sector experts to assist in the public debate, and he agrees with a number of things in the report:

- o need to balance strong security in commerce and U.S. industry's strong international presence within law enforcement and national security concerns;
- o agrees that improvement is needed and acknowledged that export controls be relaxed, not eliminated;
- o goal is that if key recovery is assumed, there would be no restrictions on algorithms or key length;
- o key escrow is not fully tested and may create unknown technical risks to cryptography;
- o more optimistic than the NRC report at this juncture; and,
- o agrees with more testing and investment in government products to do testing.

McConnell said that the emphasis was on data transmission and voice and that there were definite concerns about the storage vs. data transmission criteria performance requirements. The working group hopes to have a second draft document available by mid-July.

Information Assurance/Critical Information Infrastructure

Mr. Michael Vatis, Associate Deputy Attorney General, Department of Justice briefed the board on the efforts of a working group to a develop a policy for critical information

infrastructure to deal with threats such as physical attacks, conventional or unconventional. There are more than just physical terrorists attacks. There are cyber vulnerabilities in computer/communications systems by hackers, organized crime, foreign intelligence/powers, etc. The infrastructure would look at network systems of industry, public and private, and identify those that were vital and how their destruction /unavailability would seriously impact the country. These would include industry involving such areas as telecommunication services, electric-gas oriented suppliers, transportation, water supply, emergency services such as fire and rescue. This group realizes that policy cannot be developed by the government alone. The vulnerable civilian infrastructures are privately owned, therefore, industry's cooperation is needed. They team began meeting in December of 1995 with representatives from DOD, Justice, Transportation, Energy, and NSC. Their goal is to prepare an unclassified report identifying recommendations for legislation, government structure as well as the establishment of a Presidential commission to handle specifically defined tasks. This commission would include industry experts. They are not recommending that a new agency be developed.

Cryptography's Role in Securing the Information Society

Herb Lin, Senior Staff Officer and Study Director for the National Research Council, Computer Science and Telecommunications Board Study of National Cryptography Policy, discussed the study and its recommendations. The study was to assess the effect of cryptographic technologies on national security interests and law enforcement interests of the U.S. government; commercial interests of U.S. industry and privacy interests of U.S. citizens. In addition, it was to assess the effect on commercial interests of U.S. industry of export controls on cryptographic technologies. The report identified six recommendations in support of a national cryptographic policy: (1) No law should bar the manufacture, sale, or use of any form of encryption within the United States; (2) National cryptography policy should be developed by the executive and legislative branches on the basis of open pubic discussion and governed by the rule of law; (3) The policy affecting the development and use of commercial cryptography should be more closely aligned with market forces; (4) Export controls on cryptography should be progressively relaxed but not eliminated; (5)The U.S. government should take steps to assist law enforcement and national security to adjust to new technical realities of the information age; and (6) The U.S. government should develop a mechanism to promote information security in the private sector.

Electronic Benefit Transfer Security

Joe Leo, Board member, presented an overview on the electronic benefit transfer program (EBT) and the Federal Aid entitlement program run out of the Department of Agriculture.

He reported that currently there were over 42 states involved or becoming involved in the food stamp program electronic benefits transfer program. Mr. Leo stated that once EBT is fully implemented among the states, it is projected that $125 billion per year in both federal and state program funds would move thorough the system. Ron Jerome of Booz, Allen and Hamilton presented an overview of the risk management assessment being conducted of the ETB system to identify vulnerabilities, determine consequences of threats, assess risks and optimize the selection of controls to protect assets. He identified the respective tasks and deliverables of this work effort and presented a status of the efforts to date. Randy Hahn, also of Booz, Allen and Hamilton, discussed the development of a security technology demonstration for the EBT project. He said that they hope to begin test and evaluation in August with results documented in September. They also expect to identify one of the States to demonstrate the technology and have a live demonstration ready in October. Mr. Leo distributed copies of the USDA Electronic Benefit Transfer System Security Guideline to the Board members.

The meeting recessed at 4:55 p.m.

Thursday, June 13, 1996

Privacy Update

Marc Rotenberg, director of the Electronic Privacy Information Center, updated the Board on the Communications Decency Act (CDA), OECD and crypto, crypto and litigation, and privacy on the Internet. Rotenberg said that there were two challenges to the CDA citing that the decision bars enforcement of portions of the CDA which prohibit the distribution to minors of "indecent" or "patently offensive" materials over computer networks. He also cited U.S. District Judge Stewart Dalzell's concern that "As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from governmental intrusion". The Department of Justice will have to decide whether to appeal to the Supreme Court; Rotenberg feels that it likely.. He stated that the legal significance of CDA and how technological solutions cut both ways in the legal world; less restrictive alternative to government regulation yet widespread availability could make enforcement of CDA easier. Rotenberg reiterated some of the major points previously discussed by Sandra Lambert with regard to the establishment of OECD experts on crypto policy and the nine draft principles that are under consideration. He stated that the central tension in the US position regarded voluntary use vs. government access (business vs. law enforcement). Rotenberg briefed on two current crypto litigation activities: (1) Karn v. State (Applied Crypto on diskette)--DC Judge Ritchie rules that crypto is a "defense article" subject to Arms Export Control Act. Therefore, there was no judicial review of the Executive decision; and (2) Bernstein v. U.S.-- SF

Judge Patel rejected "defense article" rational rules that a computer program is "pure speech" for purpose of the First Amendment. This established significant Constitutional interest. Rotenberg said that the Karn decision was to be appealed.

Next, Rotenberg briefed on issues of privacy on the Internet. He reported that the Federal Trade Commission had held two days of hearings earlier in June with little outcome. Children's privacy (data collection and data usage) has become an issue. The Administration has no policy for consumer privacy to date nor have they responded to the European Community Data Directive. Rotenberg says that the big question is will the absence of government regulation on the Internet will lead to more privacy for consumers or less. Rotenberg said that EPIC has a Web site [www.epic.org] which would provide current updates on these activities and others.

Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1996

Brett Scott, Legislative Assistant, Office of Senator Conrad Burns, briefed the Board on the hearings before the Senate Commerce Committee held on Wednesday, June 12, 1996. Scott said that Senator Burns was very concerned about that current restrictions on the commercial sector to export software containing encryption. Burns has stated that more than half of the U.S. software revenues come from foreign sales. The Administration's policies jeopardize this most successful and fastest-growing market for U. S. companies. Scott distributed copies of testimonies presented at the June 12 hearing and indicated that there would be additional hearings held over the next several weeks moving this legislation toward a vote by Congress.

Electronic Security and the Market in Software-Based Services

George Spix, board member, presented an overview on Microsoft's view of the future of the marketplace. He gave a brief statistical analysis of recent software revenues. His views were that the "brick and mortar" type of institutions are changing to larger percentage of revenues through automation, e.g. financial/insurance institutions use of electronic documentation, signatures and confidentiality. He believes that the government could play a role and be a customer. He predicts terrific technology growth potential by major brands, ISV's and individual contributors. In response to a question on the role and effects of PKI infrastructure, Spix stated that PKI would likely be included as marketing ties are to the individual companies and their clients.

NIST ITL Test Competency Center

Lisa Carnahan of the Computer Security Division of the proposed Information Technology Laboratory (ITL) gave a presentation on the ITL Test Competency Center.

The primary focus is on conformance test research (i.e., test method development, test tool development and conformance test and metric development for emerging technologies). The Center will have both research and applied functions. Examples of organizations that could make use of the Test Center include ANSI X3 & X9, IEEE, NSA/MISSI, CC-based evaluations, ISO, ITU and special purpose affinity groups. Certificate issuing authority organizations will be standards development organizations, trade/industry associations, and government organizations. They will be responsible for accepting test results, determining conformance based on results, and issuing/providing validity to certificates. Carnahan went on to discuss the role of the accreditation body and function of the testing labs.

General Discussions

During discussion time, Board members unanimously approved the minutes of the March 1996 meeting.

Board member Rick Weingarten brought up his concern for privacy issue of the trend toward a national I.D. card. He suggested that this be considered as a topic for discussion at a future Board meeting. Also mentioned was the need for discussion of state driver's license status and a briefing on biometrics that the states would like to have.

Sandra Lambert presented a draft resolution to the membership to reflect the Board's comments and concerns on the draft study done by the Interagency Working Group on Cryptography Policy. After discussion and deliberation of the issues to be stated, the Board passed the resolution. The Board directed the Chairman to prepare an appropriate cover letter and forward this resolution to the co-chairs of the working group.

On the recommendation of board member Rick Weingarten, the board directed the Chairman to prepare a letter to Dr. Bruce Alberts, Chairman of the National Research Council, to commend the NRC and its Computer Science and Telecommunications board for the excellent work and through examination of cryptography as reflected in their recent study.

The meeting adjourned at 2:40 p.m.

Attachments
Letter to Dr. Bruce Alberts, NRC
Resolution 96-1
References:
#1 Sandra Lambert's slides
#2 Donna Dodson's slides
#3 Herb Lin's slides
#4 Ron Jerome's slides

Edward Roback
Secretary

CERTIFIED as a true and
accurate summary of the meeting

#5 Randy Hahn's slides
#6 Marc Rotenberg's slides
#7 Lisa Carnahan's slides

Willis Ware
Chairman